UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/774,720	02/09/2004	Xavier Boyen	ID-5	9562

36532   7590   06/11/2009
G. VICTOR TREYZ
870 MARKET STREET FLOOD BUILDING
SUITE 984
SAN FRANCISCO, CA 94102

EXAMINER
DOAN, TRANG T

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
06/11/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>26 May 2009</u>.

2a)☐ This action is **FINAL**.　　　　　2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-19</u> is/are pending in the application.

　　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-19</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>09 February 2004</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

　　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　　a)☐ All　b)☐ Some * c)☐ None of:

　　　　1.☐ Certified copies of the priority documents have been received.

　　　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　　　3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)

　　Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)

　　Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This action is in response to the amendment filed on 05/26/2009.

2.   Claims 1-19 are pending for consideration.

Response to Arguments

3.   Applicant's arguments with respect to claims 1-19 have been considered but are

moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of
matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the
conditions and requirements of this title.

4.   Claims 1-19 are rejected under 35 U.S.C. 101 because the claimed invention is

directed to non-statutory subject matter. Based upon *In re Bilski*, 545 F.3d 943, 88

USPQ2d 1385 (Fed. Cir. 2008), this action contains a new § 101 rejection of claims 1-

19 because the claims are directed towards mental steps that can be implemented

without a computer. The test for a method claim is whether the claimed method is (1)

tied to a particular machine or apparatus, or (2) transforms a particular article to a

different state or thing. Since the method of claims 1-19 can be performed without a

particular machine or apparatus, the claims are non-statutory under 35 U.S.C. 101.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

6.   Claims 1-12 and 18-19 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Zheng (US 6396928) (hereinafter Zheng) in view of Boneh et al. (US

7113594) (hereinafter Boneh)

        Regarding claim 1, Zheng discloses an identity-based-encryption (IBE)

signcryption method in which a sender signs and encrypts a message M for a recipient,

comprising: at the sender, digitally signing and encrypting a message M in a

signcryption operation using an IBE private key of the sender SK^A and an IBE public

key of the recipient ID^B that is based on the recipient's identity to generate a ciphertext

C that is a signed and encrypted version of the message M (Zheng: column 7 lines 22-

29 and column 13 lines 34-53); sending the ciphertext C to the recipient anonymously,

wherein an attacker cannot deduce the authorship of the message from the ciphertext C

(Zheng: column 1lines 14-26); at the recipient, decrypting the ciphertext C using an IBE

private key SK^B of the recipient that corresponds to the IBE public key ID^B, wherein

decrypting the ciphertext produces an unencrypted version of the message M and an

IBE public key of the sender ID^A that corresponds to the IBE private key SK^A (Zheng:

column 14 lines 54-67); and at the recipient or at a third party, after the ciphertext has

been decrypted by the recipient, performing signature verification in an operation that is

separate from the decryption of the ciphertext, wherein performing the signature

verification comprises using the decrypted message M and the IBE public key of the

sender ID^A to prove that the sender signed the message M (Zheng: column 8 lines 12-

14 and column 11 lines 25-42).

Zheng does not disclose wherein decrypting the ciphertext produces an IBE

public key of the sender ID^A that corresponds to the IBE private key SK^A. However,

Boneh discloses wherein decrypting the ciphertext produces an IBE public key of the

sender ID^A that corresponds to the IBE private key SK^A (Boneh: column 8 lines 29-

35, column 24 line 52 through column 25 line 18 and column 25 lines 50-65).

Therefore, it would have been obvious to a person skilled in the art at the time the

invention was made to have included in Zheng the feature of Boneh as discussed above

because there remains a need for improved cryptographic methods and systems

(Boneh: column 2 lines 25-26)

Regarding claim 2, Zheng as modified discloses wherein digitally signing and

encrypting the message M comprises using the IBE private key SK^A in digitally signing

the message M to produce digital signature information and using the IBE private key

SK^A in encrypting at least a portion of the digital signature information (Zheng: column

9 lines 30-63).

Regarding claim 3, Zheng as modified discloses wherein using the IBE private key SK^A in digitally signing the message M comprises computing a commitment to a secret value and computing a corresponding decommitment (Zheng: column 9 lines 30-63).

Regarding claim 4, Zheng as modified discloses wherein using the IBE private key SK^A in encrypting the digital signature information comprises using the IBE private key to compute a symmetric key (Zheng: column 2 lines 64-67).

Regarding claim 5, Zheng as modified discloses using the symmetric key to encrypt the message (Zheng: column 8 lines 55-64).

Regarding claim 6, Zheng as modified discloses using the symmetric key to encrypt the IBE public key of the recipient, at least a portion of the digital signature information, and the message (Zheng: column 9 lines 30-63).

Regarding claim 7, Zheng as modified discloses wherein digitally signing and encrypting the message M in the signcryption operation comprises: computing a commitment to a secret value r and computing a corresponding decommitment; using the IBE private key SK^A in digitally signing the message M to produce digital signature information; and using the secret value r in encrypting the message M (Zheng: column 13 lines 34-67).

Regarding claim 8, Zheng as modified discloses wherein using the secret value r

in encrypting the message M comprises using the secret value r to compute a

symmetric key (Zheng: column 13 lines 34-67).

Regarding claim 9, Zheng as modified discloses using the symmetric key to

encrypt the message (Zheng: column 8 lines 55-64).

Regarding claim 10, Zheng as modified discloses using the symmetric key to

encrypt the IBE public key of the recipient, at least a portion of the digital signature

information, and the message (Zheng: column 9 lines 30-63).

Regarding claim 11, Zheng as modified discloses wherein digitally signing and

encrypting the message M comprises using the IBE private key SK^A in encrypting the

message M (Zheng: column 13 lines 34-67).

Regarding claim 12, Zheng as modified discloses wherein digitally signing and

encrypting the message comprises performing multiplication on an elliptic or

hyperelliptic curve (Zheng: column 14 lines 43-54).

Regarding claim 18, this claim has limitations that is similar to those of claim 1,

thus it is rejected with the same rationale applied against claim 1 above.

Regarding claim 19, Zheng as modified discloses wherein sending the ciphertext

C to the intended recipient anonymously comprises sending the ciphertext C to the

intended recipient anonymously such that the attacker cannot deduce the authorship of

the message from the ciphertext C (Zheng: column 13 lines 34-67).

7.   Claims 13-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Zheng (US 6396928) (hereinafter Zheng) in view of Rohatgi (US 6826687) (hereinafter

Rohatgi).

Regarding claim 13, Zheng discloses a method of signing and encrypting a

message M comprising (Zheng: See Figs. 3-4 and column 13 lines 34-67): obtaining an

identity-based-encryption (IBE) private key of a user (Zheng: see figure 2: encrypted

using a private key cipher with k and column 13 lines 20-53); and using a symmetric key

that is based on the IBE private key to encrypt at least one of the commitment and the

decommitment (Zheng: See Figs. 3-4 and column 13 lines 34-67).

Zheng does not disclose using the IBE private key to compute a commitment to a

secret value and a corresponding decommitment. However, Rohatgi discloses using

the IBE private key to compute a commitment to a secret value and a corresponding

decommitment (Rohatgi: column 9 line 25 through column 10 line 25). Therefore, It

would have been obvious to a person skilled art at the time the invention was made to

have included in Zheng the feature of Rohatgi as discussed above to solve the problem

of packet authentication for multicast and other scenarios requiring fast, compact digital

signature/commitment for E-commerce protocols (Rohatgi: column 6 lines 48-51).

Regarding claim 14, Zheng as modified discloses wherein using the symmetric

key to encrypt comprises: concatenating the decommitment and the message (See

Figs. 3-4 and column 13 lines 34-67); and using the symmetric key to encrypt the

concatenated decommitment and message (See Figs. 3-4 and column 13 lines 34-67).

Regarding claim 15, Zheng as modified discloses wherein using the symmetric

key to encrypt comprises: concatenating an IBE public key with the message and the

decommitment (See Figs. 3-4 and column 13 lines 34-67); and using the symmetric key

to encrypt the concatenated IBE public key, decommitment, and message (See Figs. 3-

4 and column 13 lines 34-67).

Regarding claim 16, Zheng as modified discloses wherein computing the

decommitment comprises performing multiplication on an elliptic or hyperelliptic curve

(Zheng: column 14 lines 43-54).

Regarding claim 17, Zheng as modified discloses comprising computing the

symmetric key that is based on the IBE private key by performing a bilinear pairing

calculation on an elliptic or hyperelliptic curve (Zheng: column 14 lines 43-54).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431